A5.

Europäisches Patentamt | European Patent Office | Office européen des brevets

09/823875

Bescheinigung | Certificate | Attestation

Die angehefteten Unterlagen stimmen mit der ursprünglich eingereichten Fassung der auf dem nächsten Blatt bezeichneten europäischen Patentanmeldung überein.

The attached documents are exact copies of the European patent application described on the following page, as originally filed.

Les documents fixés à cette attestation sont conformes à la version initialement déposée de la demande de brevet européen spécifiée à la page suivante.

Patentanmeldung Nr. Patent application No. Demande de brevet n°

00106809.7

CERTIFIED COPY OF PRIORITY DOCUMENT

Der Präsident des Europäischen Patentamts;
Im Auftrag

For the President of the European Patent Office

Le Président de l'Office européen des brevets
p.o.

I.L.C. HATTEN-HECKMAN

DEN HAAG, DEN
THE HAGUE, 22/03/01
LA HAYE, LE

EPA/EPO/OEB Form 1014 - 02.91

Europäisches Patentamt | European Patent Office | Office européen des brevets

Blatt 2 der Bescheinigung
Sheet 2 of the certificate
Page 2 de l'attestation

Anmeldung Nr.:
Application no.:
Demande n°: 00106809.7

Anmeldetag:
Date of filing:
Date de dépôt: 30/03/00

Anmelder:
Applicant(s):
Demandeur(s):

Mannesmann VDO Aktiengesellschaft
60388 Frankfurt am Main
GERMANY

Bezeichnung der Erfindung:
Title of the invention:
Titre de l'invention:

Verfahren zur Freischaltung einer verschlüsselten Datei

In Anspruch genommene Priorität(en) / Priority(ies) claimed / Priorité(s) revendiquée(s)

Staat: State: Pays:	Tag: Date: Date:	Aktenzeichen: File no. Numéro de dépôt:

Internationale Patentklassifikation:
International Patent classification:
Classification internationale des brevets:

G06F1/00

Am Anmeldetag benannte Vertragstaaten:
Contracting states designated at date of filing: AT/BE/CH/CY/DE/DK/ES/FI/FR/GB/GR/IE/IT/LI/LU/MC/NL/PT/SE/TR
Etats contractants désignés lors du depôt:

Bemerkungen:
Remarks:
Remarques:

Ursprünglicher Titel: Siehe Seite 1 der Beschreibung

This page blank (usptc)

Mannesmann VDO AG

Kruppstraße 105
60388 Frankfurt
VF42RS/RI-ah
4645

Beschreibung

Verfahren zur Freischaltung einer Datei

Die Erfindung betrifft ein Verfahren zur Freischaltung einer auf einem Speichermedium zusammen mit mindestens einer weiteren Datei abgespeicherten Datei zur Nutzung durch ein einziges oder eine begrenzte Anzahl von lokalen Computersystemen. Weiterhin betrifft die Erfindung ein System zur Verwaltung und Freigabe von Nutzungsrechten an Dateien.

Computerprogramme und Datenbanken werden zumeist auf einem Speichermedium, wie beispielsweise einer CD-ROM, an den Endanwender verkauft. Ein solches Speichermedium weist eine hohe Speicherkapazität auf und kann zumeist mehrere Computerprogramme, gegebenenfalls in komprimierter Form, aufnehmen. Eine solche CD-ROM kann daher einen hohen Verkaufswert aufweisen. Mit Hilfe geeigneter Geräte („CD-Brenner") ist es relativ einfach Kopien von CD-ROMs herzustellen. Kopierte CD-ROMs werden teilweise kostenlos unter Interessenten ausgetauscht oder gelangen illegal in den Handel. Es besteht deshalb ein Bedarf entsprechende Programme oder allgemeiner Dateien nur für registrierte Anwender freizugeben.

Da auf einer einzigen CD-ROM mehrere Programme oder Dateien vorhanden sein können, ist es weiterhin von Interesse nur einzelne oder eine bestimmte Anzahl von Programme für einen bestimmten Anwender freizugeben. Bei-

. . .

spielsweise kann eine CD-ROM die übliche Standardbürosoftware enthalten. Zu einer solchen Bürosoftware gehören beispielsweise ein Schreibprogramm, eine Tabellenkalkulation, ein Datenbankprogramm und ein Programm zur Erstellung von Präsentationen. Der einzelne Anwender ist aber unter Umständen nur an einem Teil der Programme interessiert, wie beispielsweise dem Schreibprogramm und der Tabellenkalkulation, während die anderen Komponenten für ihn nicht von Interesse sind. Weiterhin kann der Fall eintreten, daß ein Anwender nur an der aktualisierten Version eines dieser Programme interessiert ist, ansonsten ihm jedoch die älteren Versionen der restlichen Programme völlig ausreichen, weil er diese z.B. nur selten nutzt. Dennoch muss der Anwender in beiden Fällen unter Umständen das Gesamtpaket kaufen, da die Einzelprogramme nicht separat erhältlich sind. Der Einzelvertrieb der Programme bedeutet für den Hersteller nämlich einen erhöhten Aufwand und findet daher häufig nicht statt. Für die genannten Fälle ist es daher von Interesse, nur einzelne Programme oder Dateien einer CD-ROM für einen bestimmten Anwender zur Nutzung freizugeben. Idealerweise sollte diese Freigabe wiederum mit einem entsprechenden Kopierschutz verbunden sein, so dass nach Freigabe der Datei diese auch nur von dem registrierten und berechtigten Anwender genutzt werden kann.

Aus der EP 0 679 979 A1 ist ein Verfahren bekannt, mit dem zeitlich begrenzte Nutzungsrechte an einer Computersoftware vergeben werden. Die verschlüsselte Software wird hierzu zusammen mit einem Dateiverwaltungsprogramm zunächst auf einem Speichermedium abgespeichert. Das Speichermedium wird nun an den potentiellen Anwender verschickt. Das Dateiverwaltungsprogramm wird dann von dem Anwender in dessen Computersystem geladen. Das auf dem Speichermedium abgespeicherte Programm ist dann für dieses Computersystem zugänglich. Durch das in den Computer geladene Dateiverwaltungsprogramm ist der Zugang zu dem Programm beschränkt. Mit dem beschriebenen Verfahren kann zwar ein beschränkter Zugang zu einem Computerprogramm gewährleistet werden, jedoch ist die gezielte Freigabe nur einzelner Dateien oder Programme nicht vorgesehen.

...

Aufgabe der Erfindung ist es daher, ein Verfahren anzugeben, das zum einen sicherstellt, dass ein Computerprogramm oder eine Datei nur von einem berechtigten Anwender benutzt wird, und das zum anderen eine Freischaltung nur einzelner Programme oder Dateien eines Speichermediums für einen bestimmten Anwender erlaubt.

Eine weitere Aufgabe der Erfindung ist es, ein System zur Verwaltung und Freigabe von Nutzungsrechten an Dateien anzugeben, mit dem ein solches Verfahren ausgeführt werden kann.

Die erstgenannte Aufgabe wird erfindungsgemäß gelöst mit einem Verfahren zur Freischaltung einer auf einem Speichermedium zusammen mit mindestens einer weiteren Datei abgespeicherten und mit einer Kennung AC versehenen Datei zur Nutzung durch ein einziges oder eine begrenzte Anzahl von lokalen Computersystemen durch:

- Übermitteln einer im lokalen Computersystem abgespeicherten Gerätekennzahl ID(i-1) des Computersystems an eine Zentralstelle,
- Berechnung einer neuen Gerätekennzahl ID(i) mit der übermittelten Gerätekennzahl ID(i-1) und einem Wechselcode c in der Zentralstelle,
- Festlegung eines ersten chiffrierten Codes PIN mit der berechneten Gerätekennzahl ID(i) und einem Schlüssel k in der Zentralstelle,
- Festlegung eines zweiten chiffrierten Codes ACW mit der Kennung der freizugebenden Datei und dem Schlüssel k in der Zentralstelle,
- Übermittlung des ersten chiffrierten Codes PIN und des zweiten chiffrierten Codes ACW von der Zentralstelle an das lokale Computersystem,
- Berechnung der neuen Gerätekennzahl ID(i) in dem lokalen Computersystem aus der bisher abgespeicherten Gerätekennzahl ID(i-1) und dem in einem nicht-flüchtigen Speicher des lokalen Computersystems abgelegten Wechselcode c,
- Berechnung des Schlüssels k mit dem ersten chiffrierten Code PIN und der Gerätekennzahl ID(i),

...

- Berechnung der Kennung AC der Datei mit dem zweiten chiffrierten Code ACW und dem Schlüssel k,
- Freigabe der mit der Kennung AC versehenen Datei zur Nutzung durch das lokale Computersystem.

Bei dem erfindungsgemäßen Verfahren wird die ausschließliche Nutzung einer Datei durch einen berechtigten und registrierten Anwender insbesondere dadurch erreicht, dass die Datei verschlüsselt ist. Das Speichermedium, beispielsweise eine CD-ROM, auf der die Dateien abgespeichert sind und verteilt werden, kann somit zwar weiterhin kopiert werden, jedoch können die Dateien zunächst nur bei Kenntnis des entsprechenden Schlüssels zur Entschlüsselung der Dateien genutzt werden. Um zu verhindern, dass auch der entsprechende Schlüssel von einem berechtigten Anwender an einen unberechtigten Anwender weitergegeben wird, ist vorgesehen, dass auch der Schlüssel seinerseits nur in chiffrierter Form an den berechtigten Anwender übermittelt wird. Der chiffrierte Code, der den Schlüssel enthält, enthält weiterhin die Gerätekennzahl des berechtigten Computers. Hierdurch ist gewährleistet, dass bei Weitergabe des chiffrierten Codes, der den Schlüssel enthält, die Nutzung dieses Codes auf einem weiteren Computer mit einer anderen Gerätekennzahl ausgeschlossen ist.

In einer weiteren Ausführungsform ist vorgesehen, dass die Datei nach einmaliger Freischaltung auf einer begrenzten Anzahl von Computern nutzbar ist. Dies kann dadurch erreicht werden, dass diese Computer dieselbe Gerätekennung aufweisen oder nur Teile der Gerätekennung verwendet werden, die bei diesen Computern gleich sind.

Um nur bestimmte Dateien zur Nutzung freizugeben, ist ein zweiter Code vorgesehen, der Angaben über die freizuschaltende Datei enthält. Auch dieser zweite Code muss zunächst in dem Computersystem erst dechiffriert werden, wobei dies ebenfalls nur mit der richtigen Gerätekennzahl des Computersystems möglich ist. Eine Dechiffrierung des Codes auf einem nicht berechtigten Computersystem führt aufgrund dessen abweichender Gerätekennzahl zu ei-

nem anderen Dechiffrierergebnis und damit zu einer falschen Kennung für die freizugebende Datei. Um die Sicherheit des Verfahrens weiter zu erhöhen, ist zudem vorgesehen, dass die Gerätekennzahl bei jeder Freigabe einer Datei durch die Zentralstelle geändert wird.

Die Dateien sind auf dem Speichermedium vorzugsweise in einer logischen Dateistruktur, insbesondere in einer hierarchischen Dateistruktur, abgespeichert. Die Kennung für eine bestimmte Datei kann dann anhand der Dateistruktur in einfacher Weise angegeben werde. Insbesondere ist vorgesehen, dass die Kennung einer Datei als Vektor beschreibbar ist. Durch einen solchen Vektor kann die Position in einer hierarchischen Dateistruktur besonders einfach wiedergegeben werden. Dies kann beispielsweise dadurch geschehen, dass die Komponenten des Vektors den Pfad wiedergeben, auf dem man zu der freizugebenden Datei in der Dateistruktur gelangt. Von besonderem Vorteil ist es dabei, wenn der Vektor binäre Komponenten, also Komponenten die nur zwei Zustände aufweisen, annimmt. Die Komponenten des Vektors können dann den Weg innerhalb der hierarchischen Dateistruktur kennzeichnen, wobei beispielsweise durch den Wert 1 ein Weg freigegeben wird, während durch den Wert 0 ein Weg blockiert ist. Dies kann insbesondere auch dadurch erfolgen, dass der Vektor mindestens m Komponenten aufweist, wobei m die Anzahl der Dateien ist. Unter Dateien werden hierbei auch Dateiverzeichnisse verstanden, die selbst wiederum Dateiverzeichnisse und/oder Dateien enthalten können.

Weist eine CD-ROM somit eine Dateistruktur mit m Dateien (einschließlich der Dateiverzeichnisse) auf, so weist insbesondere jeder Vektor einer Datei m Komponenten auf, die beispielsweise mit a(1), a(2), a(3), ... a(m) bezeichnet werden. Jede dieser Komponenten a(x) bezeichnet dabei eine Datei oder ein Dateiverzeichnis. Führt der Weg zu einer bestimmten Datei D(x) in der hierarchischen Dateistruktur beispielsweise über die Dateiverzeichnisse a(2), a(5), a(9), so werden die Komponenten a(2), a(5), a(9) und a(x) mit dem Wert 1 gekennzeichnet, während alle anderen Komponenten des Vektors den Wert 0 annehmen. Die Zuordnung eines solchen Vektors zu einer bestimmten Datei

. . .

wird durch das Dateiverwaltungsprogramm vorgenommen, das im Computer abgespeichert ist. Der Vektor AC für die Kennung der freizuschaltenden Datei wird an den berechtigten Anwender, wie bereits erwähnt, in chiffrierter Form übermittelt. Der chiffrierte Code kann dabei insbesondere auch weitere Informationen, wie beispielsweise über eine zeitliche Begrenzung des Nutzungsrechts enthalten. Dies ist insbesondere dadurch möglich, dass der chiffrierte Code ebenfalls als Vektor übermittelt oder von dem Computersystem in einen Vektor umgewandelt wird, wobei der Vektor dann eine oder mehrere Komponenten mit Information über die zeitliche Begrenzung des Nutzungsrechts enthält. Hierdurch ist es zudem auf einfache Weise möglich, zunächst nur Nutzungsrechte zu Testzwecken zu einem günstigen Preis oder unentgeldlich für eine begrenzte Nutzungsdauer zu erwerben und erst danach zu entscheiden, ob die unbefristeten Nutzungsrechte an der Software erworben werden sollen.

Da die Kennung für die freizuschaltende Datei vorzugsweise als Vektor verarbeitet wird, ist es insbesondere von Vorteil, wenn auch der Schlüssel k, mit dem die Dateien verschlüsselt sind, und die Gerätekennung ID als Vektor verarbeitet werden. Die Verschlüsselung kann nach einem der bekannten Verfahren erfolgen, insbesondere nach dem Data Encryption Standard (DES) unter Verwendung eines Schlüssels mit einer Länge von 56 Bit.

Das erfindungsgemäße Verfahren kann allgemein zur Freigabe und Verwaltung von Nutzungsrechten an Dateien eingesetzt werden, jedoch kann es insbesondere dann vorteilhaft eingesetzt werden, wenn auf den Computersystemen nur eine bestimmte Art von Computerprogrammen und –dateien eingesetzt wird, da dann eine Verwaltung durch eine einzige Zentralstelle leichter zu verwirklichen ist. Besonders vorteilhaft kann das Verfahren deshalb beispielsweise für die Freigabe von Nutzungsrechten an Programmen und Dateien für Navigationscomputer in Kraftfahrzeugen eingesetzt werden. In solchen Navigationssystemen werden neben Straßenkartendaten und Reiseführern auch weitere Anwendungsprogramme wie beispielsweise zur Zuordnung von Nummerierungen von Autobahnanschlußstellen zu geographischen Daten und dergleichen

...

verwendet. Aufgrund der großen Speicherdichte von CD-ROMs und insbesondere der neueren DVDs können auf einem einzelnen Speichermedium beispielsweise alle Straßenkarten der Länder Europas und die entsprechenden Reiseführer dieser Länder untergebracht werden. Ein solcher Datenträger stellt zum einen einen vergleichsweise hohen Wert dar, zum anderen benötigt nicht jeder Anwender alle Daten. Beispielsweise kann es sein, dass ein Anwender nur die Straßenkartendaten seines Heimatlandes benötigt, weil er nie mit dem eigenen Kraftfahrzeug im Ausland unterwegs ist. Ein anderer Anwender wiederum bereist dagegen neben dem Heimatland auch die angrenzenden Länder mit dem eigenen PKW regelmäßig, so dass er auch die Straßenkartendaten dieser Länder sowie die Reiseführer und/oder Hoteldatenbanken oder dergleichen benötigt.

Mit dem erfindungsgemäßen Verfahren können für die unterschiedlichsten Nutzungswünsche somit Freigaben für die Dateien gegeben werden, so dass jeder Anwender zunächst einmal nur die Nutzungsrechte für die für ihn zunächst wichtigen Regionen kauft. Hat ein Anwender nun zusammen mit dem Navigationssystem beispielsweise nur die Nutzungsrechte an den Landkartendaten für sein Heimatland erworben, so sind mit dem Kauf dieser Nutzungsrechte die Gerätekennzahl des entsprechenden Navigationssystems und vorzugsweise auch die Information über die bereits gekauften Nutzungsrechte in der Zentralstelle hinterlegt. Im Navigationssystem selbst abgespeichert ist ebenfalls die Gerätekennzahl und ein Wechselcode c. Will der Anwender nun seine Nutzungsrechte auf die Straßenkartendaten eines weiteren Landes ausdehnen, so setzt er sich mit der Zentralstelle in Verbindung und teilt dieser neben seinen Erkennungsdaten seinen Wunsch und die Art der Zahlung, beispielsweise seine Kreditkartennummer, mit. Die Zentralstelle, die die Gerätekennzahl ID(i) dieses Anwender kennt, berechnet zunächst mit dem ebenfalls in der Zentralstelle abgespeicherten Wechselcode c eine neue Gerätekennzahl ID(i). Anschließend wird in der Zentralstelle ein erster chiffrierter Code PIN mit der berechneten Gerätekennzahl ID(i) und dem Schlüssel k zur Entschlüsselung der Datei festgelegt. Anschließend wird in der Zentralstelle ein zweiter chiffrierter Code ACW

...

mit der Kennung der freizugebenden Datei und dem Schlüssel k festgelegt. Bei den chiffrierten Codes handelt es sich um numerische Codes, die insbesondere auch in dezimaler Form an den Anwender übermittelt werden können. In letzterem Fall werden nach der Übermittlung der dezimalen Codes an den Anwender und nach Eingabe der Codes in das Navigationssystem die dezimalen Codes zunächst in binäre Codes umgewandelt, wobei die einzelnen Stellen des binären Codes die Komponenten eines Vektors sind. Im Navigationssystem wird zunächst die neue Gerätekennzahl ID(i) aus der bisher abgespeicherten Gerätekennzahl ID(i-1) und dem in einem nicht-flüchtigen Speicher des lokalen Computersystems abgelegten Wechselcode c berechnet. Anschließend wird in einem weiteren Berechnungsschritt mit dem ersten chiffrierten Code PIN und der neu berechneten Gerätekennzahl ID(i) der Schlüssel k berechnet. In einem weiteren Schritt wird mit dem Schlüssel k und dem zweiten chiffrierten Code ACW die Kennung AC der freizugebenden Datei berechnet. Anschließend wird von dem Dateiverwaltungssystem die Datei mit der Kennung AC zur Nutzung durch das Navigationssystem freigeschaltet.

Ein erfindungsgemäßes System zur Verwaltung und Freigabe von Nutzungsrechten an Dateien, das zur Durchführung des erfindungsgemäßen Verfahrens geeignet ist, beinhaltet die folgenden Komponenten:

- eine Vielzahl von lokalen Computersystemen, wobei jedes der Computersysteme durch eine im Computersystem abgespeicherte Gerätekennzahl ID identifizierbar ist,
- Speichermedien für die lokalen Computersysteme, auf denen mindestens zwei Dateien abgespeichert und mit einer Kennung AC versehen sind,
- eine Zentralstelle mit einem zentralen Computersystem, in dem die Gerätekennzahlen ID der lokalen Computersysteme registriert sind, wobei zur Freigabe von Nutzungsrechten an einer Datei für eines der lokalen Computersysteme in der Zentralstelle Mittel zur Festlegung eines ersten und eines zweiten chiffrierten Codes (PIN bzw. ACW) vorhanden sind, wobei mindestens einer der Codes die abgespeicherte Gerätekennzahl des loka-

...

len Computersystems und mindestens einer der Codes die Kennung AC der freizuschaltenden Datei enthält,

- Mittel zur Übermittlung der chiffrierten Codes an das lokale Computersystem,
- Mittel zur Dechiffrierung der übermittelten Codes in dem lokalen Computersystem unter Einbeziehung der im lokalen Computersystem abgespeicherten Gerätekennzahl und zur Freischaltung der Datei zur Nutzung durch das lokale Computersystem.

Um mehrere Dateien auf einem einzigen Speichermedium unterbringen zu können, muss dieses eine ausreichend große Speicherkapazität aufweisen. Als besonders vorteilhafte Speichermedien werden insbesondere eine CD-ROM oder eine DVD angesehen. Die Dateien können aber auch auf der Festplatte des lokalen Computers in verschlüsselter Form abgespeichert sein. In diesem Fall kann die Übertragung der Dateien beispielsweise über das Internet erfolgt sein.

In einer besonderen Ausführungsform ist vorgesehen, dass der erste und der zweite chiffrierte Code direkt von der Zentralstelle in das lokale Computersystem übermittelbar sind. Diese Übermittlung kann sowohl drahtgebunden als auch drahtlos erfolgen, wobei in beiden Fällen vorzugsweise das bestehende Kommunikationsnetz, also ein Telefonfestnetz oder ein Mobilfunknetz, eingesetzt werden. Der Anwender kann dann direkt in seinem Computersystem die gewünschte Datei auswählen und diese Auswahl zusammen mit den benötigten Zahlungsdaten über das Telefonnetz oder über das Internet an die Zentralstelle übermitteln. Die Übermittlung der chiffrierten Codes erfolgt dann auch von der Zentralstelle direkt in das Computersystem über das Telefonnetz oder das Internet. Hierdurch kann eine sehr schnelle und automatisierte Freigabe von Nutzungsrechten realisiert werden. Die Nutzungsrechte werden somit über die an sich bekannten Systeme für elektronischen Handel freigeschaltet. Die Übermittlung des Freischaltungswunsches und der chiffrierten Codes kann aber

...

auch in herkömmlicher Weise durch ein Telefongespräch oder durch Übermittlung per Briefpost erfolgen.

In einer besonderen Ausführungsform ist vorgesehen, dass die Codes auf einem kostengünstigen Speichermedium geringer Dichte, wie beispielsweise einer IC-Card, abgespeichert sind, wodurch durch einfaches Einführen der IC-Card in ein entsprechendes Lesegerät des Computersystems die Codes in das Computersystem eingegeben werden und eine manuelle Eingabe entbehrlich ist.

In einer weiteren besonderen Ausführungsform, die insbesondere für Kraftfahrzeuganwendungen und damit für Navigationssysteme von Interesse ist, kann die Eingabe der Codes auch durch Spracheingabe erfolgen.

Die Erfindung wird nachfolgend anhand eines Ausführungsbeispiels und der Zeichnung näher erläutert. Es zeigen:

Fig. 1: eine Systemübersicht,

Fig. 2: die Dateistruktur der Dateien,

Fig. 3: verschiedene Varianten der Kennung der freizuschaltenden Datei,

Fig. 4: eine Systemübersicht für ein automatisiertes Freigabeverfahren,

Fig. 5: ein Ablaufdiagramm des Verfahrens.

Figur 1 zeigt eine Systemübersicht mit einer Zentralstelle 1 und sieben Computern 2a bis 2f von insgesamt n Computern. Bei den Computern 2 handelt es sich um lokale Computersysteme unterschiedlichster Art. Die Computer 2 sind mit der Zentralstelle 1 nicht über ein festes Leitungsnetz verbunden. Es ist jedoch möglich, dass die Computer 2 mit der Zentralstelle 1 über eine Telefon- oder Internetverbindung Kontakt aufnehmen. Aber auch dies ist keine Voraussetzung zur Durchführung des Verfahrens.

In der Zentralstelle 1 sind neben den Gerätekennungen ID1 bis IDn der Schlüssel k zur Entschlüsselung der verschlüsselten Dateien sowie der Wechselvektor

...

c zum Verändern der Gerätekennung ID bei jeder Freigabeprozedur als Vektoren abgespeichert. In jedem der lokalen Computer 2 ist neben der individuellen Gerätekennung ID auch der Wechselvektor c abgespeichert. Ein Softwarepaket ist auf einer CD-ROM abgespeichert und enthält mehrere Programme und Datenbanken in einer hierarchischen Dateistruktur. Weiterhin ist auf der CD-ROM ein Dateiverwaltungsprogramm abgespeichert.

In Figur 2 ist eine solche Dateistruktur dargestellt, wobei die Dateien D01 bis D18 auch Dateiverzeichnisse sein können und somit weitere Dateien oder Dateiverzeichnisse enthalten. Im Falle einer CD-ROM für ein Navigationssystem kann es sich bei der Datei D01 beispielsweise um das Dateiverzeichnis „Länder" handeln. Bei den Dateien D02 bis D04 kann es sich in diesem Fall um regionale Dateiverzeichnisse handeln, insbesondere um einzelne Länder. Diese Dateiverzeichnisse können weiter aufgespalten sein, wie dies beispielsweise bei dem Dateiverzeichnis D02 der Fall ist, das in die Dateiverzeichnisse D05 und D06 aufspaltet. Beispielsweise kann es sich bei D02 um ein Länderverzeichnis „Deutschland" handeln und bei den Dateiverzeichnissen D05 und D06 um die Dateiverzeichnisse für „Nord- bzw. Süddeutschland". Den jeweiligen Dateiverzeichnissen D05 und D06 sind dann Dateien für die Landkartendaten D12 bzw. D14 und Dateien D13 bzw. D15 mit den zugehörigen Reiseführern zugeordnet. Bei D03 kann es sich um ein Dateiverzeichnis für ein weiteres Land, beispielsweise Frankreich, handeln, wobei nunmehr diesem Dateiverzeichnis direkt die entsprechenden Dateien D07 bis D09 zugeordnet sind und es sich beispielsweise um Dateien für die Landkartendaten, einen Reiseführer und ein Hotelverzeichnis handeln kann. Jeder dieser Dateien ist eine Kennung zugeordnet, die 18 Komponenten aufweist und damit der Gesamtsumme der Dateien bzw. Dateiverzeichnisse entspricht. Das Dateiverzeichnis D01 ist dabei durch die erste Komponente des Vektors, das Dateiverzeichnis D02 durch die zweite Komponente und allgemein die Datei m durch die Komponente m des Vektors gekennzeichnet. Der gesamte Vektor für die Kennung einer Datei setzt sich nun aus dem Weg zusammen, der zu dieser Datei führt. Dies wird am Beispiel der Datei D15 beschrieben und ist in Fig. 2 im unteren Bereich dargestellt.

...

Der Weg zu der Datei D15 führt über die Dateien bzw. Dateiverzeichnisse D01, D02, D06 und D15, so dass im zugehörigen Vektor für die Datei D15 die entsprechenden Positionen 01, 02, 06 und 15 den Wert 1 annehmen, während alle anderen Komponenten des Vektors den Wert 0 annehmen. Um einen ausreichenden Schutz der Kennung einer Datei zu gewährleisten, sollte diese aus nicht zu wenigen Komponenten bestehen. Um auch bei einer geringen Anzahl von Dateien einen ausreichenden Schutz durch die Kennung zu gewährleisten, kann diese erweitert werden, wie dies in Fig. 3 dargestellt ist.

In Figur 3a ist eine Kennung mit 10 Komponenten dargestellt, wobei dies der Anzahl der Dateien entsprechen soll. In Fig. 3b ist eine Erweiterung dieser Kennung auf 19 Komponenten dargestellt, wobei zwischen den eine Datei kennzeichnenden Komponenten Zufallskomponenten r eingefügt sind, die durch das System wieder eliminiert werden.

Der Nutzer eines der Computer 2 kann nun eine CD-ROM mit mehreren Dateien käuflich erwerben, wobei er zunächst noch keine endgültigen Nutzungsrechte erwerben muss. Beispielsweise erwirbt der Käufer eines Neuwagens zugleich mit diesem ein Navigationssystem und eine CD-ROM mit den zugehörigen Datenbanken. Da der Anwender jedoch u.U. als solcher in der Zentralstelle noch nicht registriert ist, hat er mit seinem Computersystem auch noch keinen Zugang zu den einzelnen Dateien, die auf der CD-ROM verschlüsselt abgelegt sind. Zunächst wird der Anwender das Dateiverwaltungssystem, das ebenfalls auf der CD-ROM abgespeichert ist, in sein Computersystem laden. Anschließend muss sich der Anwender von der Zentralstelle die Nutzungsberechtigung einholen. Hierzu kann der Anwender mit der Zentralstelle telefonisch Kontakt aufnehmen.

Im weiteren soll jedoch ein automatisiertes Verfahren beschrieben werden, das die in Figur 4 dargestellten Komponenten nutzt. Hierbei handelt es sich neben dem lokalen Computer 2 und der Zentralstelle 1 um ein Vermittlungsmedium 3, das mit beiden verbunden ist. Die Verbindung zwischen der Zentralstelle 1 und dem Computersystem 2 kann dabei beispielsweise über eine Festnetztelefon-

...

verbindung mittels eines Modems, einer ISDN- oder einer ADSL-Leitung erfolgen. Es kann sich weiterhin um eine Funkverbindung mit einem Mobilfunktelefon und einer Datenübertragung nach dem WAP-Standard handeln, oder die Datenübertragung kann über das Mobilfunktelefon als SMS-Nachricht erfolgen. Als weiteres Beispiel wird eine Datenübertragung über das Internet genannt.

Das erfindungsgemäße Verfahren selbst wird nachfolgend anhand der Figur 5 näher erläutert.

Der Computernutzer ruft im Schritt S1 zunächst ein Menuprogramm auf, das ihm eine Auswahl über die auf der CD-ROM abgespeicherten Programme und Datenbanken auflistet. Der Anwender wählt eines oder mehrere der gewünschten Programme aus und gibt zusätzlich die erforderlichen Angaben zu den Zahlungsmodalitäten, wie beispielsweise seine Kreditkartennummer, ein (Schritt S2). Anschließend aktiviert der Anwender den Sendeaufruf, mit dem die Verbindung zur Zentralstelle aufgerufen wird. In Schritt S4 erfolgt schließlich die Herstellung der Verbindung zur Zentralstelle, beispielsweise über eine Mobilfunkverbindung im Falle eines Kraftfahrzeugnavigationssystems oder auch über eine Internetverbindung. Anschließend erfolgt im Schritt S5 die Übertragung des Freischaltungswunsches, der Zahlungsdaten, sowie der gegenwärtigen Gerätekennung $\underline{ID}(i-1)$, die in einem nicht-flüchtigen Speicher des Computers abgelegt ist und automatisch mit übermittelt wird.

Nach Empfang dieser Daten berechnet die Zentralstelle zunächst eine neue Gerätekennung $\underline{ID}(i)$ aus der bisherigen Gerätekennung $\underline{ID}(i-1)$ und dem Wechselvektor $\underline{c}$, beispielsweise: $\underline{ID}(i) = \underline{ID}(i-1)^*\underline{c}$.

Anschließend wird ein erster chiffrierter Code $\underline{PIN}$ berechnet, der die neue Gerätekennung $\underline{ID}(i)$ und den für die Verschlüsselung der Dateien der CD-ROM erforderlichen Schlüssel $\underline{k}$ enthält, beispielsweise gemäß: $\underline{PIN} = inv[\underline{ID}(i)]^*\underline{k}$.

Anschließend wird ein zweiter chiffrierter Code $\underline{ACW}$ berechnet, der den Schlüssel $\underline{k}$ sowie die Kennung $\underline{AC}$ für die gewünschte freizuschaltende Datei enthält (Schritt S6), beispielsweise gemäß: $\underline{ACW} = \underline{k} * \underline{AC}$.

...

In Schritt S7 werden die neue Gerätekennung ID(i) sowie eine Information über die freigeschaltete Datei und die Zahlungsmodalitäten in der Zentralstelle abgespeichert.

Anschließend werden die chiffrierten Codes PIN und ACW an den lokalen Computer zurückübertragen, und die Verbindung wird beendet. Im Falle der geschilderten automatischen Freigabe können die chiffrierten Codes PIN und ACW direkt als Vektoren bzw. Binärzahlen übermittelt werden.

Im Falle einer Freigabe durch ein Telefongespräch oder auf dem Postwege ist es vorteilhaft, wenn der Vektor, der binäre Komponenten enthält, zunächst als Binärzahl geschrieben und in eine Dezimalzahl umgewandelt wird, wobei dann die Dezimalzahl an den Anwender übermittelt wird. Der Anwender kann in diesem Fall die einfachere und kürzere Dezimalzahl in sein Computersystem eingeben, das dann wiederum die Umwandlung in eine Binärzahl bzw. in einen Vektor mit binären Komponenten vornimmt.

Das im Computer nach Übermittlung oder Eingabe der Codes PIN und ACW ablaufende Verfahren ist ebenfalls in Fig. 5 in den Schritten S10 bis S14 dargestellt. Zunächst wird im Computersystem die neue Gerätekennung ID(i) aus der bisher im Gerät abgespeicherten bisherigen Gerätekennung ID(i-1) und dem ebenfalls im Computersystem abgespeicherten Wechselvektor c berechnet gemäß: $\underline{ID}(i) = \underline{ID}(i-1)*\underline{c}$.

Mit der neuen Gerätekennung ID(i) und dem ersten chiffrierten Code PIN kann nun der Schlüssel k zur Entschlüsselung der Dateien berechnet werden. Anschließend wird mit dem Schlüssel k bzw. dem zu dem Schlüsselvektor k inversen Vektor inv(k) und dem zweiten chiffrierten Code ACW die Kennung AC der freizuschaltenden Datei berechnet gemäß: $\underline{AC} = inv(\underline{k})*\underline{ACW}$. Für symmetrische Verschlüsselungsalgorithmen ist $inv(\underline{k}) = \underline{k}$.

Das Dateiverwaltungssystem gibt nun die zu der Kennung AC gehörende Datei zur Nutzung frei und diese kann über den nunmehr bekannten Schlüssel k ent-

...

schlüsselt werden und zur Anzeige gebracht oder zur weiteren Bearbeitung genutzt werden.

Bei dem erfindungsgemäßen Verfahren ist somit die Freigabe einer Datei immer an die Gerätekennung gekoppelt, so dass die Freigabecodes nicht für ein anderes System genutzt werden können. Durch die bei jeder neuen Freigabe einer Nutzungsberechtigung vorgenommene Änderung der Gerätekennung wird eine erhöhte Sicherheit erreicht. Die Dateien auf dem Datenträger sind zudem mit dem Schlüssel k verschlüsselt, wobei der Schlüssel k aus dem ersten chiffrierten Code PIN nur bei Kenntnis der Gerätekennung erzeugt werden kann. Die Kennung AC der freizuschaltenden Datei wiederum kann aus dem zweiten chiffrierten Code erst bei Kenntnis des Schlüssels k berechnet werden.

Mit dem erfindungsgemäßen Verfahren kann weiterhin auch eine zeitlich befristete Freigabe von Dateien realisiert werden. Eine solche zeitlich befristete Freigabe ist beispielsweise von Interesse, um eine Software für wenige Tage zu testen und erst nach dem Test zu entscheiden, ob ein volles Nutzungsrecht erworben werden soll. In einem solchen Fall kann für einen geringen Preis die CD-ROM mit den Dateien erworben werden und die Dateien können über die Zentralstelle für einen befristeten Zeitraum von beispielsweise 3 Tagen oder einer Woche freigeschaltet werden. Auch bei Kraftfahrzeugnavigationssystemen ist eine befristete Freigabe von Interesse, z. B. dann wenn ein Anwender nur für einen beschränkten Zeitraum Landkartendaten eines bestimmten regionalen Bereichs benötigt. Hierbei kann es sich beispielsweise um einen einmaligen Auslandsurlaub in einem Land X für wenige Wochen handeln.

Eine solche zeitlich befristete Freigabe einer Datei kann dadurch erreicht werden, dass die Kennung der freizuschaltenden Datei Komponenten enthält, die eine zeitlich befristete Freigabe kennzeichnen. Eine entsprechende Kennung ist beispielsweise in Fig. 3c dargestellt. In diesem Beispiel sind die ersten 10 Komponenten des Vektors AC für die Kennung mit den auf der CD-ROM abgespeicherten Dateien wie in den zuvor beschriebenen Fällen verknüpft. Weiterhin enthält der Vektor nun aber die Komponenten t1, t2 und t3, die Hinweise

...

auf eine zeitlich beschränkte Nutzung geben. Beispielsweise kann über die Komponente t1 eine Freigabe der Datei für einen Zeitraum von einer Woche gegeben sein, wenn diese Komponente auf 1 gesetzt ist. Entsprechend kann über die Komponente t2 eine Freigabe für einem Zeitraum von einem Monat gegeben sein, wenn diese Komponente auf 1 gesetzt ist. In entsprechender Weise kann über die Komponente t3 die Freischaltung für einen Zeitraum von 6 Monaten vorgegeben werden. Der Zeitraum beginnt dabei erst mit der Freischaltung der Datei zu laufen. Das Computersystem bzw. das Dateiverwaltungsprogramm des Computersystems erkennt dabei, ob eine der Komponenten t1 bis t3 auf eins gesetzt wurde, und setzt eine entsprechende Zeitmarke, wobei bei jeder geplanten neuen Nutzung der Datei geprüft wird, ob der gesetzte Zeitrahmen abgelaufen ist.

Mannesmann VDO AG

Kruppstraße 105
60388 Frankfurt
VF42RS/RI-ah
4645

Patentansprüche

1. Verfahren zur Freischaltung einer auf einem Speichermedium zusammen mit mindestens einer weiteren Datei abgespeicherten und mit einer Kennung AC versehenen Datei zur Nutzung durch ein einziges oder eine begrenzte Anzahl von lokalen Computersystemen durch:

   - Übermitteln einer im Computersystem abgespeicherten Gerätekennzahl ID(i-1) des Computersystems an eine Zentralstelle
   - Berechnung einer neuen Gerätekennzahl ID(i) mit der übermittelten Gerätekennzahl ID(i-1) und einem Wechselcode c in der Zentralstelle
   - Festlegung eines ersten chiffrierten Codes PIN mit der berechneten Gerätekennzahl ID(i) und einem Schlüssel k in der Zentralstelle
   - Festlegung eines zweiten chiffrierten Codes ACW mit der Kennung der freizugebenden Datei und dem Schlüssel k in der Zentralstelle,
   - Übermittlung des ersten chiffrierten Codes PIN und des zweiten chiffrierten Codes ACW von der Zentralstelle an das lokale Computersystem
   - Berechnung der neuen Gerätekennzahl ID(i) in dem lokalen Computersystem aus der bisher abgespeicherten Gerätekennzahl ID(i-1) und dem in einem nicht-flüchtigen Speicher des lokalen Computersystems abgelegten Wechselcode c

. . .

- Berechnung des Schlüssels k mit dem ersten chiffrierten Code PIN und der Gerätekennzahl ID(i)
- Berechnung der Kennung AC der Datei mit dem zweiten chiffrierten Code ACW und dem Schlüssel k,
- Freigabe der mit der Kennung AC versehenen Datei zur Nutzung durch das lokale Computersystem.

2. Verfahren nach Anspruch 1, dadurch gekennzeichnet, dass die Dateien mit dem Schlüssel k verschlüsselt sind und zur Nutzung durch das Computersystem mit dem Schlüssel k entschlüsselt werden.

3. Verfahren nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass die Dateien auf dem Speichermedium in einer logischen Dateistruktur, insbesondere in einer hierarchischen Dateistruktur, abgespeichert sind.

4. Verfahren nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass die Kennung einer Datei als Vektor beschreibbar ist.

5. Verfahren nach Anspruch 4, dadurch gekennzeichnet, dass der Vektor binäre Komponenten aufweist.

6. Verfahren nach Anspruch 4 oder 5, dadurch gekennzeichnet, dass der Vektor mindestens m Komponenten aufweist, wobei m die Anzahl der Dateien ist.

7. Verfahren nach Anspruch 6, dadurch gekennzeichnet, dass über m Komponenten a(1), a(2), a(3), ... des Vektors AC(x)=(a(1), a(2), a(3), ..., a(x-1), a(x), a(x+1), ..., a(m)) die Position einer Datei D(x) in der hierarchischen Dateistruktur derart bestimmt wird, dass alle Komponenten des Vektors AC(x), die Dateien zugeordnet sind, von denen die Datei D(x) hierarchisch abhängig ist, einen ersten Wert, insbesondere den Wert 1, annehmen, während alle verbleibenden Komponenten, die Dateien zugeordnet sind, von

...

denen die Datei D(x) hierarchisch nicht abhängig ist, einen zweiten Wert, insbesondere den Wert O, annehmen.

8. Verfahren nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass der Schlüssel k als Vektor beschreibbar ist.

9. Verfahren nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass die Gerätekennung ID als Vektor beschreibbar ist.

10. Verfahren nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass es sich bei dem Computersystem um einen Navigationscomputer eines Kraftfahrzeug-Navigationssystems handelt.

11. Verfahren nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass die Dateien Straßenkartendaten enthalten.

12. Verfahren nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass die Dateien Anwendungsprogramme enthalten.

13. Verfahren nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass einer der chiffrierten Codes eine Information über eine zeitliche Begrenzung des Nutzungsrechts enthält.

14. Verfahren nach Anspruch 13, dadurch gekennzeichnet, dass der zweite chiffrierte Code als Vektor beschreibbar ist und der Vektor eine oder mehrere Komponenten enthält, in der die Information über die zeitliche Begrenzung der Nutzungsdauer abgelegt ist.

15. Verfahren nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass die Vektoren der chiffrierten Codes vor der Übermittlung in Dezimalzahlen umgewandelt werden.

16. Verfahren nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass die Datei(en) über ein Kommunikationsnetz an das Computersystem übermittelt wird (werden).

...

17. System zur Verwaltung und Freigabe von Nutzungsrechten an Dateien, das die folgenden Komponenten beinhaltet:

- eine Vielzahl von lokalen Computersystemen (2a bis 2n), wobei jedes der Computersysteme (2) durch eine im Computersystem (2) abgespeicherte Gerätekennzahl ID identifizierbar ist,
- Speichermedien für die lokalen Computersysteme (2), auf denen mindestens zwei Dateien abgespeichert und mit einer Kennung AC versehen sind,
- eine Zentralstelle (1) mit einem zentralen Computersystem, in dem die Gerätekennzahlen ID der lokalen Computersysteme registriert sind, wobei zur Freigabe von Nutzungsrechten an einer Datei für eines der lokalen Computersysteme in der Zentralstelle Mittel zur Festlegung eines ersten und eines zweiten chiffrierten Codes (PIN bzw. ACW) vorhanden sind, wobei mindestens einer der Codes die abgespeicherte Gerätekennzahl des lokalen Computersystems und mindestens einer der Codes die Kennung AC der freizuschaltenden Datei enthält,
- Mittel zur Übermittlung der chiffrierten Codes an das lokale Computersystem (2),
- Mittel zur Dechiffrierung der übermittelten Codes in dem lokalen Computersystem (2) unter Einbeziehung der im lokalen Computersystem (2) abgespeicherten Gerätekennzahl und zur Freischaltung der Datei zur Nutzung durch das lokale Computersystem (2).

18. System nach Anspruch 17, dadurch gekennzeichnet, dass es sich bei den Speichermedien um optische Speichermedien, insbesondere CD-ROM oder DVD handelt.

19. System nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass es sich bei den lokalen Computersystemen (2) um Navigationscomputer in Kraftfahrzeug-Navigationssystemen handelt.

...

20. System nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass das lokale Computersystem (2) ein Dateiverwaltungssystem enthält, das nur solche Dateien zur Nutzung freigibt, zu denen die Kennung AC vorliegt.

21. System nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass der erste und der zweite chiffrierte Code direkt von der Zentralstelle (1) in das lokale Computersystem übermittelbar ist.

22. System nach Anspruch 21, dadurch gekennzeichnet, dass die Übermittlung drahtlos erfolgt.

23. System nach Anspruch 21 oder 22, dadurch gekennzeichnet, dass das lokale Computersystem (2) mit einem Funktelefon verbunden ist.

24. System nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass die Dateien verschlüsselt sind.

25. System nach einem der vorhergehenden Ansprüche, gekennzeichnet durch Mittel zum Übertragen der Dateien von der Zentralstelle zu dem lokalen Computersystem.

26. System nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass der Schlüssel k zur Entschlüsselung der Dateien in einem der chiffrierten Codes enthalten ist.

27. System nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass es für elektronischen Handel der Nutzungsrechte ausgelegt ist.

28. System nach einem der vorhergehenden Ansprüche, gekennzeichnet durch ein tragbares Speichermedium geringer Dichte, insbesondere eine IC-card, auf dem der erste und der zweite Code abgespeichert sind.

. . .

Mannesmann VDO AG

Kruppstraße 105
60388 Frankfurt
VF42RS/RI-ah
4645

Zusammenfassung

Verfahren zur Freischaltung einer Datei

Es wird ein Verfahren zur Freigabe von Nutzungsrechten an einer auf einem Speichermedium zusammen mit mindestens einer weiteren Datei abgespeicherten und mit einer Kennung versehenen Datei zur Nutzung durch ein einziges oder eine begrenzte Anzahl von lokalen Computersystemen beschrieben.

Hierzu wird von einer Zentralstelle ein erster und ein zweiter chiffrierter Code PIN bzw. ACW berechnet, der einen Schlüssel k zur Entschlüsselung der verschlüsselt abgespeicherten Dateien und eine Gerätekennzahl ID enthält. Die Gerätekennzahl ID wird bei jeder neuen Freigabe geändert. Nach Eingabe der beiden chiffrierten Codes in das Computersystem wird in diesem zunächst eine neue Gerätekennzahl ID aus abgespeicherten Daten und mit dieser neuen Gerätekennzahl ID und dem ersten chiffrierten Code PIN des Schlüssel k und mit dem Schlüssel k und dem zweiten chiffrierten Code ACW eine Kennung AC der freizuschaltenden Datei berechnet.

Figur 5

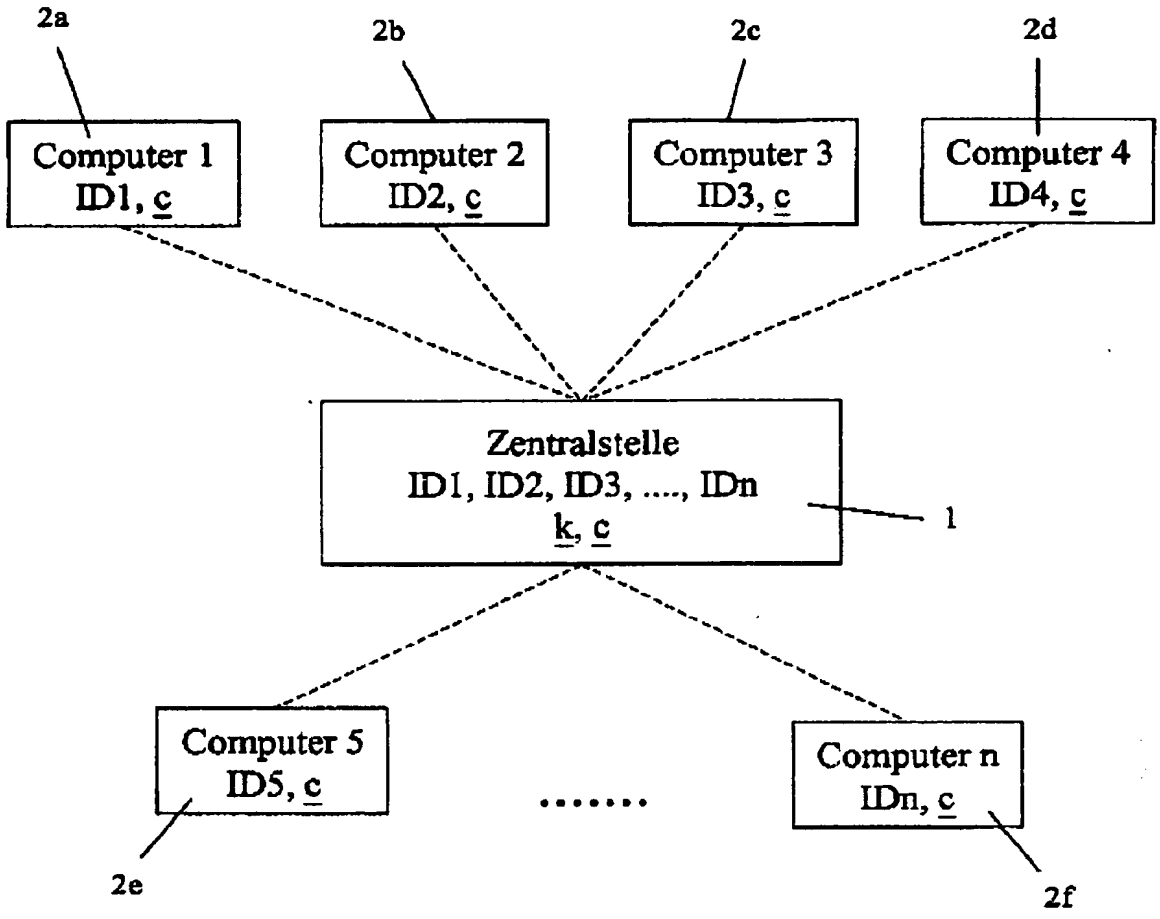
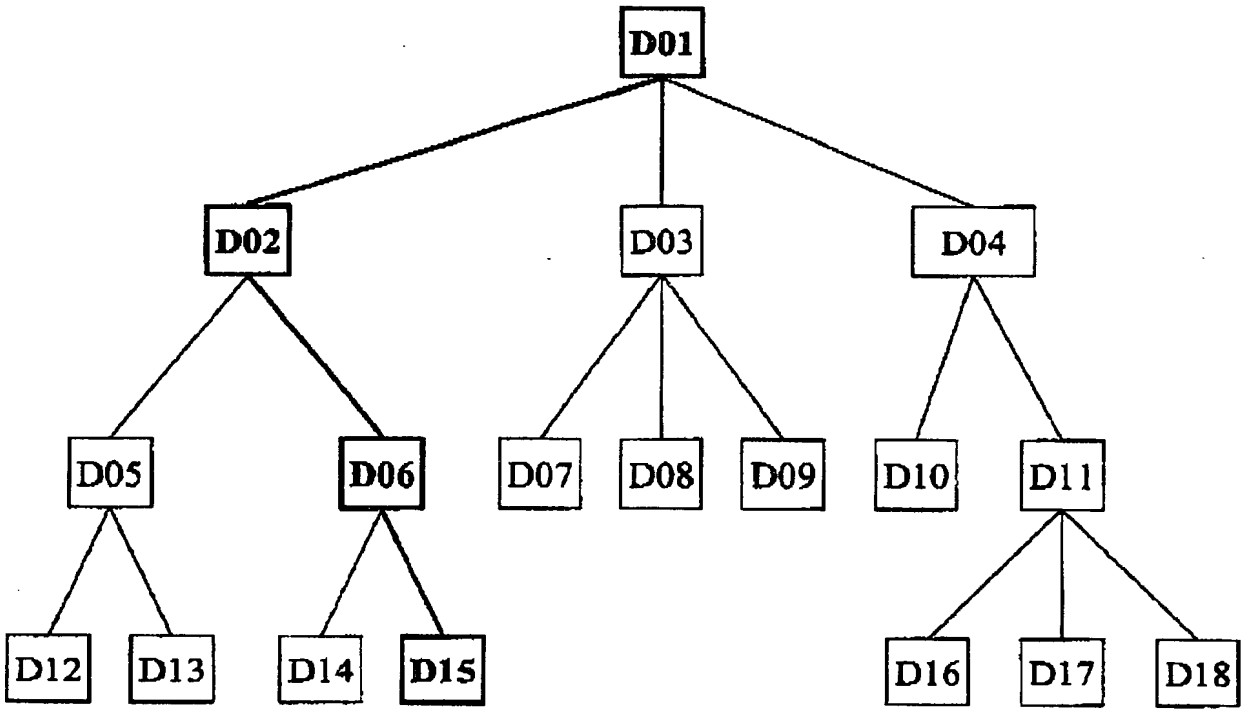

2a
2b
2c
2d
Computer 1
ID1, c
Computer 2
ID2, c
Computer 3
ID3, c
Computer 4
ID4, c
Zentralstelle
ID1, ID2, ID3, ..., IDn
k, c
1
Computer 5
ID5, c
.....
Computer n
IDn, c
2e
2f

Fig. 1



Nr: **01 02** 03 04 05 **06** 07 08 09 10 11 12 13 14 **15** 16 17 18

AC: **1** 1 0 0 0 1 0 0 0 0 0 0 0 0 1 0 0 0

Fig. 2

Nr: 01 02 03 04 05 06 07 08 09 10

AC: 1 1 0 0 0 1 0 0 0 0

a)

Nr: 01 r 02 r 03 r 04 r 05 r 06 r 07 r 08 r 09 r 10

AC: 1 1 1 0 0 1 0 0 0 1 1 0 0 0 0 1 0 0 0

b)

Nr: 01 02 03 04 05 06 07 08 09 10 t1 t2 t3

AC: 1 1 0 0 0 1 0 0 0 0 0 1 0

c)

Fig. 3

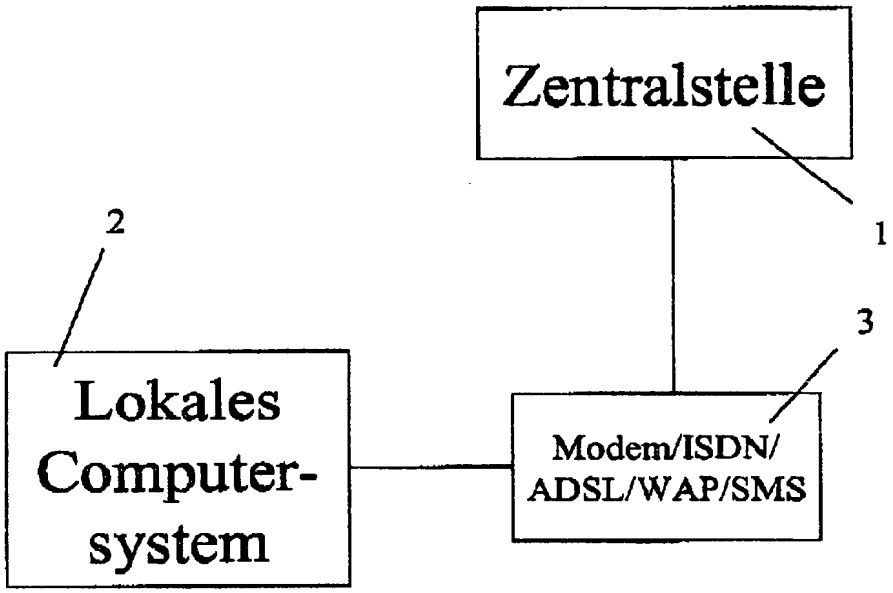

Zentralstelle
1
2
3
Lokales Computer-system
Modem/ISDN/ ADSL/WAP/SMS

Fig. 4

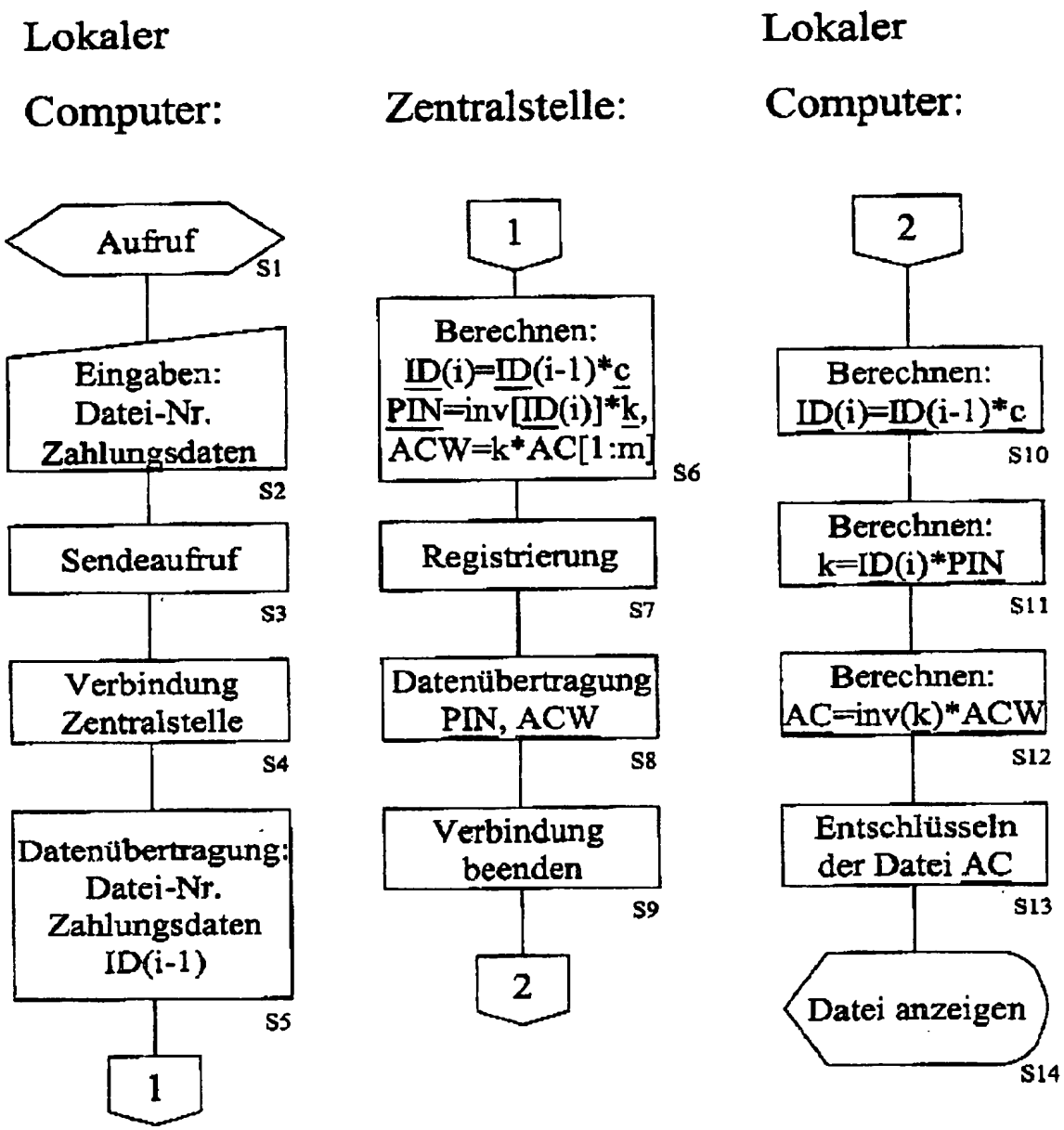

Lokaler Computer:
Zentralstelle:
Lokaler Computer:
Aufruf
S1
Eingaben: Datei-Nr. Zahlungsdaten
S2
Sendeaufruf
S3
Verbindung Zentralstelle
S4
Datenübertragung: Datei-Nr. Zahlungsdaten ID(i-1)
S5
1
1
Berechnen: ID(i)=ID(i-1)*c PIN=inv[ID(i)]*k, ACW=k*AC[1:m]
S6
Registrierung
S7
Datenübertragung PIN, ACW
S8
Verbindung beenden
S9
2
2
Berechnen: ID(i)=ID(i-1)*c
S10
Berechnen: k=ID(i)*PIN
S11
Berechnen: AC=inv(k)*ACW
S12
Entschlüsseln der Datei AC
S13
Datei anzeigen
S14

Fig. 5